NIS DIRECTIVE EXPLAINED

Alan Levine *reveals how all the attention on the GDPR deadline means that the implications of the Networks and Information Systems Directive may have fallen by the wayside*

The much-anticipated wait for the General Data Protection Regulation (GDPR) finally came to an end on the 25 May of this year. Over the last 18 months, both pre and post the GDPR implementation, businesses have been overwhelmed with advice and guidance on how to comply, but arguably many companies still have a long way to go before they reach compliance. However, in comparison, not much fuss has been made about another critical regulation that was launched two weeks before the GDPR on 9 May: The NIS (Networks and Information Systems) Directive.

The NIS Directive is not something to be sniffed at. While it does not apply to everyone that handles EU resident data as the GDPR does, it still affects a significant number of UK businesses. The Directive targets organisations defined as "essential services," whose reliability and security are essential to the continuation of everyday activities. These organisations are further defined by the Centre for the Protection of National Infrastructure (CPNI) as: "…(facilities, systems, sites, property, information, people, networks and processes), the loss or compromise of which would result in major detrimental impact on the availability, delivery or integrity of essential services, leading to severe economic or social consequences or to loss of life". NIS, therefore, affects a range of businesses including those that supply electricity, water, gas, healthcare, emergency services, passenger and freight transport and digital services among others.

> **ORGANISATIONS NEED TO PUT SYSTEMS IN PLACE TO RAISE THEIR OVERALL LEVELS OF CYBER SECURITY**

Furthermore, the NIS Directive arguably has a wider scope than the GDPR. In contrast to the GDPR's data privacy focus, NIS aims to address the overall cyber security state of critical services. According to the UK's NCSC (National Cyber Security Centre – part of the GCHQ), the NIS Directive is necessary because: "These systems can be an attractive target for malicious actors… there is therefore a need to improve the security of network and information systems across the UK… which if disrupted, could potentially cause significant damage to the economy, society and individuals' welfare". In order to ensure compliance, essential services organisations need to put systems and processes in place that raise their overall levels of cyber security, improve the resilience of their network and information systems, and generally create an internal culture of security.

The Directive has been designed to establish common standards for preparedness, co-operation, response, and security awareness across the EU. The directive is aimed at member states as a whole, as well as specific operators of essential services within those states. Operators are responsible for their own compliance. The objectives of the NIS Directive have been designed to improve cross-border co-operation in respect to information and network security, as well as to develop an EU-wide culture of risk management.

KEY REGULATIONS

The NIS Directive sets out a number of key regulations for affected organisations to abide by. Firstly, it states that operators of essential services are responsible for their own compliance. However, member states should encourage businesses to develop thorough response and recovery measures, security awareness education programs and risk assessment plans. Secondly, operators of essential services must take appropriate action to develop an EU-wide culture of risk management, including implementing security awareness training. Thirdly, operators of essential services are required to take appropriate technical and organisational measures to secure their network and information systems and minimise the impact of security incidents. And lastly, if any significant security incidents do occur, operators are required to notify local CSIRTs (Computer Security Incident Response Teams) and other relevant bodies "without undue delay". Overall the regulation endeavours to improve EU and broader international co-operation in information and network security.

In the shadow of GDPR, the NIS Directive is seemingly not getting the attention it rightly deserves. NIS fines are comparable to those of the GDPR, with non-compliance costing organisations between €10 million and €20 million, or 2-4 percent of an organisation's annual global turnover. Despite this, due to a lack of preparedness, it was recently revealed in a freedom of information request that 70 percent of UK critical infrastructure organisations could be liable for fines under the NIS Directive, and if maximum fines were to be imposed it could cost the UK economy more than £2.5 billion. And it doesn't stop there. If critical service organisations also work with EU resident data, then they are still required to comply with the GDPR as well, which means that they could face two sets of monumental fines.

This may seem extreme, but with the continuously evolving threat landscape and the rising risk of nation state cyber attacks, I'd argue that governments are right to push more stringent cyber regulations. There really is no choice.

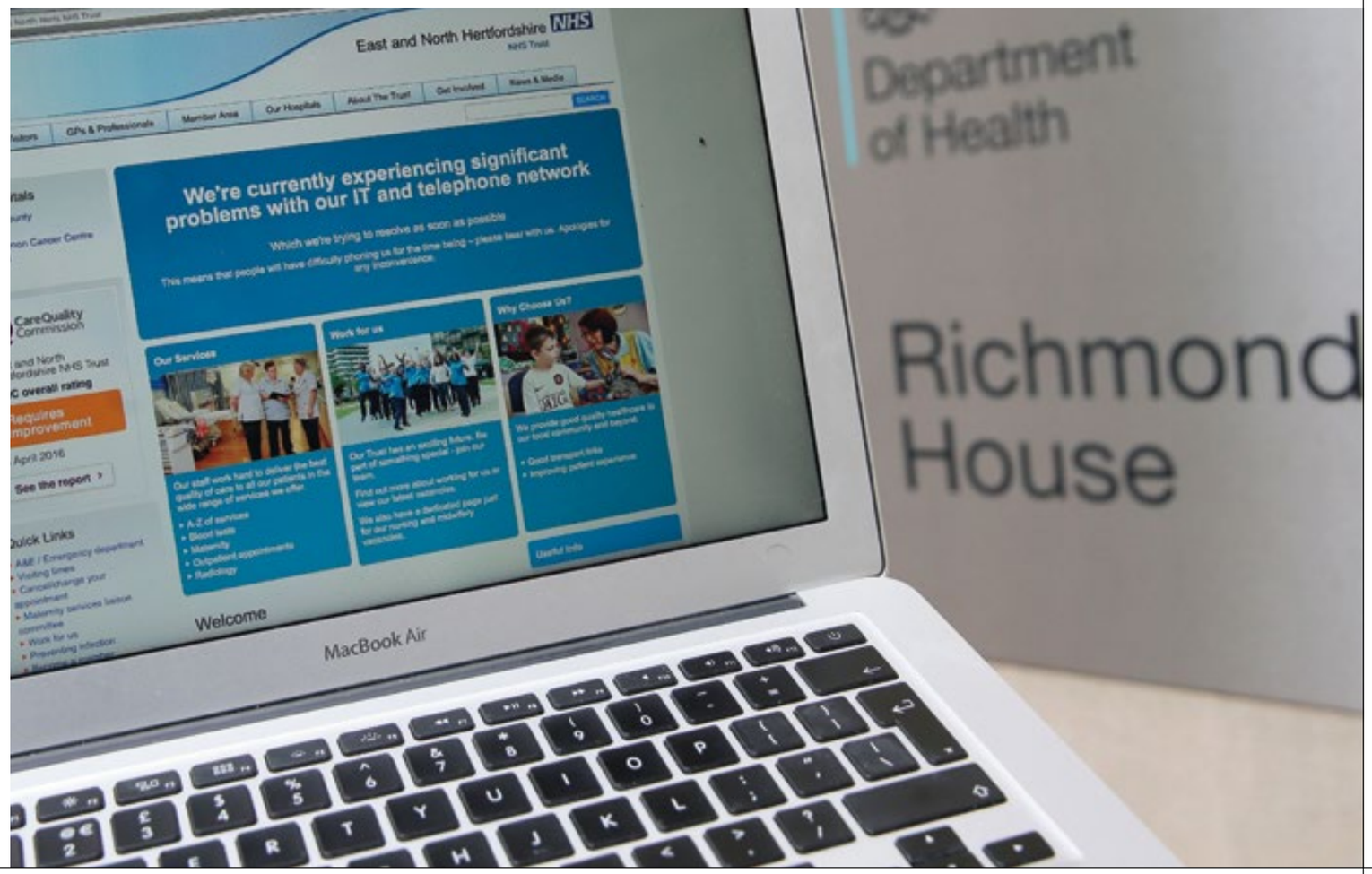
It is an unfortunate truth that today's cyber threat landscape is so bleak that we need such stringent regulations such as the NIS Directive. For example, just recently, the 12 of May marked one year since the prolific WannaCry attack occurred. The first reports of the outbreak came from the National Health Service in the UK. 80 out of the 236 NHS trusts across England suffered disruptions, as well as another 603 NHS organisations, including 595 GP practices. Staff were having to revert to using paper and pens when seeing patients, and some also made use of their personal mobile phones, exposing organisations to additional cyber risk. And still over a year on, a report issued by the Public Accounts Committee in April this year found that the NHS' cyber resilience was not up to standard. New announcements from the NHS, including that it will be investing £150 million to bolster its cyber security and a new Enterprise Agreement with Microsoft, are great steps forward. But only time will tell if it has done enough to protect itself against cyber attacks and if it is measuring up to the NIS Directive's stringent regulations.

The NotPetya attack of June 2017 also had serious repercussions for critical infrastructure. Not only was shipping giant Maersk hit by the attack, resulting in a loss of $300 million, but Ukraine was also severely impacted. Ukraine's national bank, a state power company and largest airport all fell victim to NotPetya, and residents were unable to use ATMs, fill up their cars with petrol or complete other everyday tasks that ensure business as usual. The country's economy and the population's quality of life were affected by this attack, evidence of the serious nature of what's at stake.

The effects of falling victim to a cyber attack are only likely to get worse and will impact organisations at all levels, internally and via the supply chains they support and depend upon. Therefore, the NIS Directive shouldn't just be the concern of IT and security departments – it is vital for C-level leadership and board members to also understand its expectations. Ultimately, if an organisation is found to be non-compliant, and thus less secure than it should be, all related critical services may be impacted.

When comparing the GDPR and the NIS Directive, the NIS stands out because it explicitly sets forth

In May 2017 the NHS suffered from the WannaCry ransomware attack, bringing chaos to hospitals across the UK



Picture credit: Getty

requirements for education, awareness and training programs relating to network and information security. Security awareness is required both on member-state and organisational levels, as one of the objectives of the NIS Directive is to develop an EU-wide culture of risk management. This needs to be promoted "downwards" from the EU, but organisations must also play a part from the ground up by educating employees on how to spot and respond to cyber threats.

In fact, Verizon's 2018 Data Breach Investigations Report (DBIR) revealed that organisations are almost three times more likely to get breached by social attacks than via vulnerabilities in technology. This was illustrated during the NotPetya attack when hackers accessed corporate networks via phishing emails that targeted users. Imagine if, due to a lack of cyber security awareness in your organisation, one of your users clicked on a link in an email that helped to launch the next global cyber attack?

BEST PRACTICES FOR ALL

Every company is unique; utility companies and hospitals have very different operational models, for example. However, there are several common best practices that all organisations should consider when implementing security awareness training. Organisations should ensure that they have buy-in and participation from all levels. It goes without saying that to develop a culture of risk management and cyber security within an organisation they need executive and board-level support. Board members and C-suite executives are ultimately role models for the rest of the business, so if they are seen to be cyber aware and supporting the cyber security cause, this will lay the foundation for developing an internal culture that helps to protect the company.

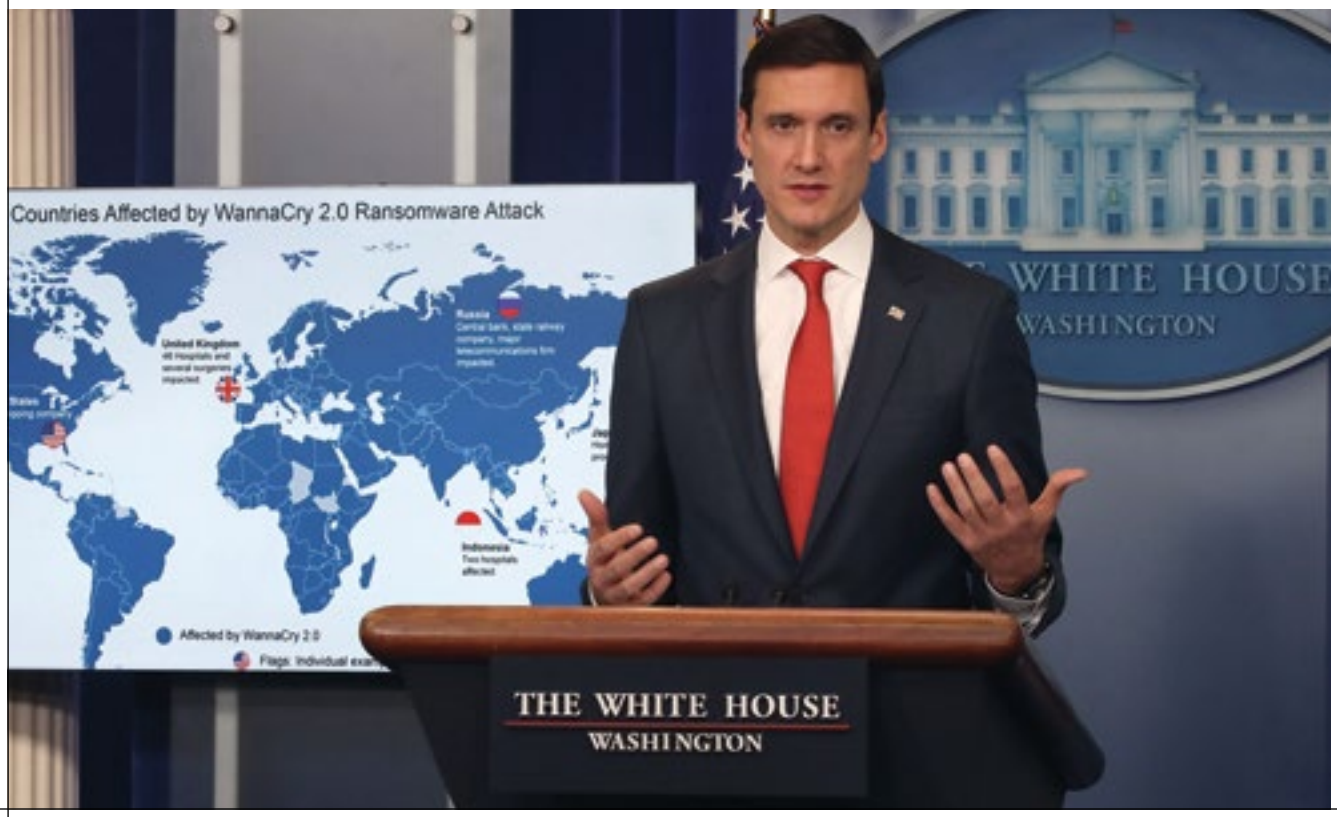
Furthermore, businesses shouldn't patronise employees by keeping them out of the loop. A clear internal communications strategy is useful for myriad reasons, including developing a culture of cyber security. A message should come from leadership before a user training initiative starts, giving them background on why it is important and what it will consist of. Communications should continue throughout a campaign so that employees never need to question why they are participating in it.

Before starting a training campaign, it is important to gauge employees' susceptibility to phishing, measure levels of cyber security knowledge and identify important metrics like the rates of malware infections and successful phishing attacks from the wild. These baseline vulnerability measures allow you to mark your starting point and monitor progress effectively from there.

Organisations also need to make sure they implement regular, ongoing assessments and training. To change mindsets and reduce the mistakes and risk associated with end-user behaviours, cyber security must become a regular pursuit. Occasional phishing tests and once or twice-a-year training simply will not be enough to raise awareness and help employees learn how to apply best practices. To develop new skills, users must be given the benefit of regular cyber security education and the opportunity to learn over time.

Those organisations that are classified as 'essential services' need to ensure that they are bolstering their cyber security defences, not only to comply with the NIS Directive but also to defend against the evolving threat landscape. As suggested in the directive itself, businesses need to utilise their last line of defence: their employees. By giving employees a seat at the security table, they will be more likely to actively engage in cyber security best practices and contribute that much-needed last layer of protection. Furthermore, every business is essential to someone, so all businesses should take note of the NIS Directive and its requirements. The Directive is setting a standard that we should all follow. In order to properly defend against cyber attacks, we need a virtual army of employees who can recognise and report attacks, in order to stop the plague of cyber criminals in their tracks ●

Alan Levine is a security advisor to Wombat Security with extensive global experience. He specialises in all facets of cyber security and global data privacy with an emphasis on European privacy provisions, and compliance, including SOX and related corporate compliance requirements.



Homeland Security advisor Tom Bossert holds a White House briefing on countries affected by the WannaCry cyber attack

Picture credit: Getty